



**Small Business Administration
Automated Information Systems Security Program**

PRIVACY IMPACT ASSESSMENT FOR

***(STANDARD 7(A) LOAN GUARANTY
PROCESSING SYSTEM)***

SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

Name of Project: Standard 7(a) Loan Guaranty Processing System
Program Office: Office of Capital Access

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- SBA IT Security Manager
- SBA OCIO IT Portfolio Division
- SBA Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Jeffrey Browning
Center Information Resource Manager
Office of Capital Access
262 Black Gold Blvd.
Hazard, KY 41701
606-436-0801 Ext. 233

2) Who is the System Owner?

Frank Pucci
Center Director for 7(a) Loan Guaranty Processing
6501 Sylvan Road
Citrus Heights, CA 95610
(916) 735-1969

3) Who is the System Manager for this system or application?

Jeffrey Browning
Center Information Resource Manager
7(a) LGPC
Office of Capital Access
Jeffrey.browning@sba.gov
262 Black Gold Blvd.

Hazard, KY 41701
606-436-0801 Ext. 233

4) Who is the IT Security Manager who reviewed this document?

David McCauley
Chief Information Security Officer
Office of the Chief Information Officer
David.McCauley@sba.gov
202-205-7103

5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

Ethel Matthews
Senior Advisor to the Chief Privacy Officer
Office of the Chief Information Officer
Ethel.Matthews@sba.gov
202-205-7173

6) Who is the Reviewing Official?

Christine H. Liu
Chief Information Officer/ Chief Privacy Officer
Office of the Chief Information Officer
Christine.Liu@sba.gov
202-205-6708

B. PIA PROCESS APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual!?

Yes

b. Is the information about individual members of the public?

Yes

c. Is the information about employees?

No

2) What is the purpose of the system/application?

The Standard 7(a) Loan Guaranty Processing System consists of processes required for processing Standard 7(a) Loans. These processes result in collection of information from Standard 7(a) Loan Applications.

3) What legal authority authorizes the purchase or development of this Process?

Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, §§1701-1710 (1998) (codified as 44 U.S.C.A. § 3504 n. (West Supp. 1999)).

C. DATA IN THE PROCESS

1) What categories of individuals are covered in the system/application?

Information will be acquired and retained on Standard 7(a) Loan Applicants.

2) What are the sources of the information in the Standard 7(a) Loan Guaranty Processing System?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, source then what other source?

Information in the system is derived from the individuals applying for a Standard 7(a) Loan Guaranty.

b. What Federal agencies are providing data for use in the process?

None

c. What State and local agencies are providing data for use in the process?

None

d. From what other third party sources will data be collected?

Credit Scoring information is obtained from Fair Isaac Corporation.

e. What information will be collected from the employee and the public?

The system collects the user login ID of the employee using the system to make any update/change/input of data to the system.

The system will collect following information on the loan applicant:

- Name (Last, First, Middle Initial and Suffix)

- Social Security Number (SSN)
- Address (Street, City, State and Zip)

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than SBA records be verified for accuracy?

Current 7(a) Loan Guaranty Application information is verified by lender contact.

b. How will data be checked for completeness?

Both visual verification and internal software controls.

c. Is the Data Current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Applicant Information is verified by lender contact and SBA employee review and verification; if data is not current an employee makes necessary contacts to obtain current information.

d. Are the data elements described in detail and documented?

Yes, Etrans Data Model was used in the standardization of data elements.

D. ATTRIBUTES OF THE DATA

1) Is the use of the data both relevant and necessary to the purpose for which the process is being designed?

Yes

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

Credit score information will be obtained from Fair Isaac and stored electronically in the Microsoft SQL Server DBMS and an electronic copy of the credit information will reside on the File Server. Information is filed in the systems electronic loan file; it does not generate new data.

3) Will the new data be placed in the individual's record?

The credit score information will be collected and maintained in the applicant's SQL Record.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No. Credit Information is a critical process in Loan Processing.

5) How will the new data be verified for relevance and accuracy?

The credit information is obtained through major credit bureaus and includes personal information that results in a positive match with our records.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The systems are functioning within the SBA Firewall and also have internal software controls in place to identify users and assign security permissions to prevent unauthorized access. The individual servers also have a active configured firewall in place.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.

Yes, the system functions within the SBA Firewall and uses a HTTPS Connection with VeriSign Digital Certification Authentication for communication with FairIsaac LiquidCredit.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

The unique identifier for personal information is generated by the DBMS and is not part of the applicant's personal information.

- 9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The system produces reports for LGPC staff only, reports are those necessary for loan guaranty decision-making and/or statistical information for HQ i.e. the number of Small/Rural Lender Advantage (S/RLA) loans processed in a specific week.

- 10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

These options would be through the 7(a) Loan Guaranty Application, either on the SBA Form 4 or the SBA Form 2301.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

- 1) **If the information in the process operated in more than one site, how will consistent use of the data be maintained in all sites?**

The information is used with the LGPC site only.

- 2) **What are the retention periods of data in the system?**

SBA's Privacy Act System of Records, SBA 21 procedures will be used.

- 3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept?**

Where SBA's Privacy Act System of Records, SBA 21 procedures will be used.

- 4) **Are the systems in the process using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

- 5) **How does the use of this technology affect public/employee privacy?**

The information on applicants is sensitive in nature and should be protected from unauthorized access.

- 6) **Will this system in the process provided the capability to identify, locates, and monitor individuals? If yes, explain.**

No. The system has the capability to only retrieve and store applicant information.

- 7) **What kinds of information are collected as a function of the monitoring of individuals?**

No individual monitoring occurs with the system.

- 8) **What controls will be used to prevent unauthorized monitoring?**

The system functions with the SBA Firewall and uses internal software controls to identify users and prevent unauthorized access.

- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name?**

SBA Privacy Act System of Records SBA 21

- 10) **If the system is being modified, will the Privacy Act Systems of records notice require amendment or revision? Explain.**

N/A

F ACCESS TO DATA

- 1) **Who will have access to the data in the System? (E.g. contractors, users, managers, system administrators, developers, tribes, other).**

LGPC staff are the only users of the system, based on need to know login access.

- 2) **How is access to the data by a user determined? Are criteria, procedures, controls and responsibilities regarding access documented?**

The user is verified by internal software controls and assigned security levels based on userid.

- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Users will be restricted based on the assigned security level for each user.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

This would not apply since LGPC staff have access to all Standard 7(a) Loan Information. Information could potentially be deleted by a number of staff members, however we have system audit trails and any change to anything in the system is date stamped to the second and who made the change.

- 5) Are contractors involved with the design and development of the: system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

No

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

No

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The LGPC Information Resource Staff.

- 8) Will other agencies share data or have access to the data in this system?**

No.

- 9) How will the data be used by the other agency?**

NA

- 10) Who is responsible for assuring proper use of the data?**

Frank Pucci, Center Director 7(a) LGPC

G. PRIVACY IMPACT ANALYSIS

- 1) Discuss what privacy risks were identified and how they were mitigated for types of information collected.**

Because the system will collect some PII information and not everyone needs to have access to the information, only those that need to know the EIN or SSN information will be able to view it. Also, only those that need to know queries based on EIN or SSN will have permission to do so, through control of access privileges within the system.

- 2) Describe any types of controls that may be in place to ensure that information is used as intent.**

Users will have to sign a rules of behavior document. SBA will predetermine roles for users in the system which means that specific forms will be made available to a user depending on their job function at the SBA.

- 3) Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?**

The system may use extracts and lockboxes. Only required data will be exchanged. Electronic data will be transferred using a secure interface including, VPN, secure lease line, file encryption, secure shell, digital certificate authentication, SSL and secure FTP.

A user's access will be based on the responsibility assigned to the user. Therefore, users' access will be restricted by responsibility. The predetermined responsibilities- as described in the question above -assign different forms and types of data to a user.

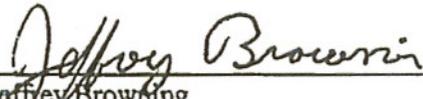
- 4) What privacy risks were identified and describe how they were mitigated for security and access controls?**

To ensure employees do not view PII data not required in the performance of their jobs, user accounts will be assigned specific roles and responsibilities. Users will be limited in their access to areas of the system appropriate for those responsibilities.

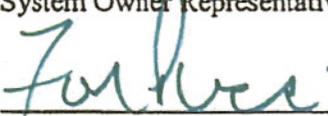
SIGNATURE PAGE

The following officials have approved this document:

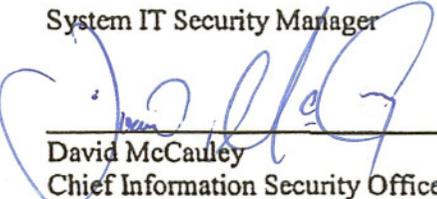
System Program Manager

 _____ (Signature) 12-1-08 (Date)
Jeffrey Browning
Center IRM

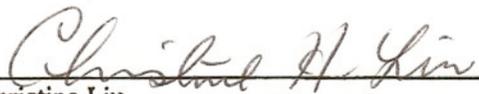
System Owner Representative

 _____ (Signature) 12/1/08 (Date)
Frank Pucci
Center Director

System IT Security Manager

 _____ (Signature) 12/17/08 (Date)
David McCauley
Chief Information Security Officer

System Privacy Official

 _____ (Signature) 1/5/09 (Date)
Christine Liu
Chief Information Officer/ Chief Privacy Officer